REMARKS

Response is hereby made to the Office Action dated December 18, 2003. By this Response, Applicant has not amended the claims, so claims 1-18 remain pending the application. *Although no fee or extension of time is believed to be required by this Response, the Commissioner is authorized and requested provide any extensions of time and/or to debit any fees that may be required by this Response (including any fees for additional claims or extensions of time) from Deposit Account No. 50-2091 to avoid abandonment of this Application.*

The Office Action rejects claims 1-13 and 15-17 under 35 USC § 102(b), citing US Patent No. 5,153,919 ("Reeds"). The Office Action rejects claims 14 and 18 under 35 USC § 103, citing the combination US Patent No. 5,432,852 ("Leighton") with the Reeds reference. Applicant respectfully traverses the rejections in that neither reference fails to disclose or suggest each and every element of the amended claims, taken singly or in combination. In particular, no reference of record discloses at least:

> *determining memory range information identifying a range of memory space within the remote unit having data to be hashed by a hashing function*

or

> *determining position information indicative of a position within a data stream to be generated within the remote unit at which said random value is to be located.*

The present invention relates to a technique for identifying tampering in a remote subscriber device such as a cable box. To determine if a legitimate subscriber has tampered with the device to obtain unauthorized services, the invention creates a "hash" digest of a random portion of the device's memory. To prevent hackers from breaking this scheme, the hash is created with a random number seed and using a portion of the device's memory that varies from trial to trial. After the device computes the hash, it places the result in a location in memory /data stream that also varies. Accordingly, the claimed method involves producing three data values (a random number, a memory range, and a position in the data stream for storing the random number) and providing each of these data values to the remote device for

6

processing. This variation and randomness in the various parameters serves to thwart unscrupulous users. Again, this technique is particularly useful for identifying tampering within the remote device, since the contents of the device's memory are used to create the hash resultant.

Unlike the present invention, the Reeds system is not concerned with identifying tampering in the remote device, but rather is concerned with authenticating portable phones to a service provider to prevent unauthorized access to a wireless network. Because Reeds is concerned with unauthorized access rather than tampering, the system described in the reference exploits a completely different technique for accomplishing its own results. To that end, Reeds describes a system whereby access is granted based upon a digital signature provided by the phone (*see* Reeds FIG. 2 and accompanying text). This signature is computed based upon the device's electronic serial number ("ESN"), a secret key ("A-key") provided by the service provider when the phone is initialized, and a random number ("RANDSSD") provided by the service provider at various intervals. The phone receives the random number and creates "shared secret data" (SSD) that can be duplicated and verified by the service provider. Note, however, that the only information provided from the service provider to the device when conducting a query is the RANDSSD value. There is no other data relating to memory range information or a position in a data stream that is processed within the system, let alone delivered to the remote unit.

Reeds therefore does not describe *determining memory range information* *identifying a range of memory space within the remote unit having data to be hashed by a hashing function*, nor does it describe *determining position information indicative of a position within a data stream to be generated within the remote unit at which said random value is to be located* as recited by independent claim 1. Independent claims 8 and 15 similarly recite memory range information and a position in a data stream, so the above analysis applies to these claims as well. Indeed, Reeds would have no used for functionality found in applicant's claims, since Reeds is concerned with authentication rather that with verifying the contents of the memory of the device. The Leighton reference similarly fails to provide the elements of Applicant's claims not found in Reeds.

7

Because each of the dependent claims inherit the restrictions of their parent independent claims, these claims are believed to be patentable a fortiori, and a detailed analysis of the patentability of these claims is not required at this time. Nevertheless, Applicant does not consent to any of the rejections found in the Office Action, and expressly reserves the right to separately dispute the patentability of any dependent claim at a later date, if necessary to do so.

In view of the above analysis, no reference (nor any combination of references) expressly or impliedly discloses each and every aspect of Applicant's claims. Applicant has addressed each of the concerns set forth in the Office Action, and all of the pending claims are therefore believed to be allowable. Applicant therefore respectfully requests reconsideration and withdrawal the rejections set forth in the Office Action, and allowance of each of the remaining claims. Should the Examiner have any questions or wish to further discuss this application, Applicant requests that the Examiner contact the undersigned at (480) 385-5060 or bcarlson@ifllaw.com.

Respectfully submitted,

Dated 3/31/2004
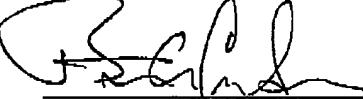
Brett A. Carlson
Reg. No. 39,928

Ingrassia Fisher & Lorenz P.C.
Customer No. 29906

8